

Parallel Time and Quantifier Prefixes

Felipe Cucker
Dept. of Mathematics
City University of Hong Kong
83 Tat Chee Avenue, Kowloon
Hong Kong

e-mail: `macucker@cityu.edu.hk`

Paulin Jacobé de Naurois
CNRS UMR 7030 - LIPN
Université Paris Nord
99 av. J.B. Clement
93430 Villetaneuse cedex
France

e-mail: `denaurois@lipn.univ-paris13.fr`

Abstract. We characterize the amount of alternation between blocks of digital quantifiers (having both existential and universal), blocks of real existential quantifiers, and blocks of real universal quantifiers that can be decided in parallel polynomial time over the reals. We do so under the assumption that blocks have a uniform bound in their size, both for the case of this bound to be polynomial and constant. As a result of this characterization (and as a stepping stone towards it) we prove a real version of Savitch Theorem.

1 Introduction

In classical complexity theory there is a neat relationship between complexity classes and quantifier prefixes preceding a predicate decidable in polynomial time. A prefix made of existential quantifiers only corresponds to the class **NP**, one made of universal quantifiers only to the class **coNP** and, more generally, one alternating k blocks of quantifiers to the class Σ_k (if the first block is of existential quantifiers) and to the class Π_k (if the first block is of

universal quantifiers). Furthermore, if one allows the (polynomial number of) quantifiers in the prefix to arbitrarily vary we obtain the class PSPACE of sets decidable in polynomial space (or, equivalently, in polynomial parallel time).

In the complexity theory over the reals developed by Blum, Shub, and Smale [3] some differences with the situation above stand out. Firstly, space in itself is not such a meaningful resource [8] and the role of the class PSPACE is played over the reals by the class $\text{PAR}_{\mathbb{R}}$ of sets decidable in polynomial parallel time. Secondly, no quantifier prefix appears to correspond with this complexity class.

Indeed, while the alternation of k blocks of quantifiers leads to the classes $\Sigma_{\mathbb{R}}^k$ and $\Pi_{\mathbb{R}}^k$ of the polynomial hierarchy $\text{PH}_{\mathbb{R}}$ over the reals [2] which is included in $\text{PAR}_{\mathbb{R}}$ [1], the unrestricted alternation of polynomially many quantifiers yields a class $\text{PAT}_{\mathbb{R}}$ (from polynomial alternating time) which strictly includes $\text{PAR}_{\mathbb{R}}$ [6]. But there is more. Call a quantifier *digital* if its argument is restricted to take values in $\{0, 1\}$. Then, it is easy to see, the class $\text{DPAT}_{\mathbb{R}}$ obtained via the unrestricted alternation of digital quantifiers is included in $\text{PAR}_{\mathbb{R}}$. A natural question arising at this moment is

Which quantifier prefixes, allowing for both digital and real quantifiers, can be solved within $\text{PAR}_{\mathbb{R}}$?

While a complete answer to this question seems elusive since sequences of quantifier prefixes can be very unstructured one can nevertheless restrict attention to quantifier prefixes possessing a certain regularity. Some results within this framework are shown in [4]. For instance, it is shown that $\text{DPAT}_{\mathbb{R}}^{\text{PH}_{\mathbb{R}}} \subseteq \text{PAR}_{\mathbb{R}}$. Furthermore, define the classes $\text{MA}\exists_{\mathbb{R}}$ (*Mixed Alternation with real Existentials*) and $\text{MA}\forall_{\mathbb{R}}$ (*Mixed Alternation with real Universals*) consisting of all the sets decidable alternating digital universal and real existential (respectively, digital existential and real universal) guesses in polynomial time. It is also shown in [4] that $\text{PAR}_{\mathbb{R}} \subsetneq \text{MA}\exists_{\mathbb{R}}$ and $\text{PAR}_{\mathbb{R}} \subsetneq \text{MA}\forall_{\mathbb{R}}$.

These results shed some light on the relations between quantifier prefixes and computations in $\text{PAR}_{\mathbb{R}}$. For, on the one hand, the class $\text{DPAT}_{\mathbb{R}}^{\text{PH}_{\mathbb{R}}}$ can be characterized by a form of alternation where one first alternates a polynomial number of digital quantifiers and then a polynomial number of real quantifiers (but these ones with only a bounded number of alternations). And, on the other hand, the classes $\text{MA}\exists_{\mathbb{R}}$ and $\text{MA}\forall_{\mathbb{R}}$ allow real quantifiers to alternate with digital ones provided all the real quantifiers are of the same kind.

A first result in this paper extends the results above by showing that $\text{PH}_{\mathbb{R}}^{\text{DPAT}_{\mathbb{R}}} \subseteq \text{PAR}_{\mathbb{R}}$. Together with the results in [4] this allows to build a whole hierarchy of complexity classes within $\text{PAR}_{\mathbb{R}}$. Define

$$\Theta_0 = \text{DPAT}_{\mathbb{R}} \text{ and } \Upsilon_0 = \text{PH}_{\mathbb{R}}$$

and, for $k > 1$,

$$\Theta_k = \text{DPAT}_{\mathbb{R}}^{\Upsilon_{k-1}} \text{ and } \Upsilon_k = \text{PH}_{\mathbb{R}}^{\Theta_{k-1}}.$$

Finally, let the *Quantifier Hierarchy* be $\text{QH}_{\mathbb{R}} = \bigcup_{k \geq 0} \Theta_k = \bigcup_{k \geq 0} \Upsilon_k$. We show that $\text{QH}_{\mathbb{R}} \subseteq \text{PAR}_{\mathbb{R}}$. This gives a complete answer on how much alternation can be decided in $\text{PAR}_{\mathbb{R}}$ if we allow both the digital blocks (themselves alternating existential and universal quantifiers), the existential real blocks, and the universal real blocks to have polynomial size.

We further extend this result to a characterization of the amount of alternation decidable in $\text{PAR}_{\mathbb{R}}$ when the size of the (three kinds of) blocks above is bounded. In this case the number of block alternations has to be at most $(\log(n))^{\mathcal{O}(1)}$.

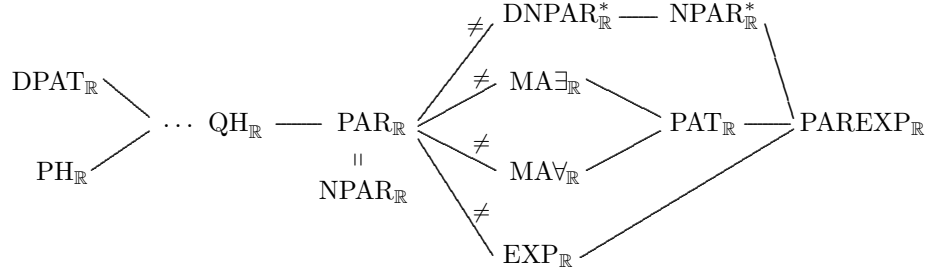
The power of quantification is also related with a well-known result in classical complexity. In [9] Savitch proved that $\text{NPSPACE} = \text{PSPACE}$. To extend this result to the real setting (besides replacing PSPACE by $\text{PAR}_{\mathbb{R}}$) requires to agree on how much nondeterminism we want to endow parallelism with. The obvious definition for a set A to be decidable in nondeterministic parallel polynomial time requires the existence of a set B deciding pairs (x, y) in parallel time polynomial in the size of x and of a function g such that, for $x \in \mathbb{R}^n$,

$$x \in A \iff \exists y \in \mathbb{R}^{g(n)} \text{ s.t. } (x, y) \in B.$$

The issue is how ‘big’ should g be. Denote by $\text{NPAR}_{\mathbb{R}}$ and $\text{NPAR}_{\mathbb{R}}^*$ the classes obtained by taking g to be a polynomial and an exponential function respectively. Using a similar notation, Savitch result shows that $\text{PSPACE} = \text{NPSPACE} = \text{NPSPACE}^*$. A main result in this paper shows that over the reals the situation differs once more since we actually have (using obvious notations)

$$\text{DNPAR}_{\mathbb{R}} = \text{NPAR}_{\mathbb{R}} = \text{PAR}_{\mathbb{R}} \subsetneq \text{DNPAR}_{\mathbb{R}}^* \subseteq \text{NPAR}_{\mathbb{R}}^*.$$

We can summarize the relationship between complexity classes emerging from our results in the following diagram (where a line means inclusion of the left-hand side class in the right-hand side one and the expressions $\text{EXP}_{\mathbb{R}}$ and $\text{PAREXP}_{\mathbb{R}}$ denote the classes of sets decidable in exponential time and parallel exponential time, respectively).



2 Preliminaries

We denote by \mathbb{R}^∞ the disjoint union of the Euclidean spaces \mathbb{R}^n , for $n \geq 1$. Given $x \in \mathbb{R}^\infty$ we denote by $|x|$ its *size*, i.e., the only $n \geq 1$ such that $x \in \mathbb{R}^n$. For a set $S \subseteq \mathbb{R}^\infty$ we write $S_n = S \cap \mathbb{R}^n$.

We consider sequential machines over \mathbb{R} as originally defined in [3] (see also [2]). As a model of parallel machine we consider P-uniform families of algebraic circuits (see [2, §18.4]). Actually, we endow the sign gates of a circuit with the function $\text{sign} : \mathbb{R} \rightarrow \{-1, 0, 1\}$ where, for $a \in \mathbb{R}$,

$$\text{sign}(a) = \begin{cases} 1 & \text{if } a > 0 \\ 0 & \text{if } a = 0 \\ -1 & \text{if } a < 0 \end{cases}$$

instead of the two-valued sign function in [2, §18.4]. These machine models allow one to define the classes $P_{\mathbb{R}}$, $NP_{\mathbb{R}}$, $NC_{\mathbb{R}}$, and $PAR_{\mathbb{R}}$ of subsets $S \subseteq \mathbb{R}^\infty$ decidable in polynomial (resp. nondeterministic polynomial, parallel polylogarithmic, and parallel polynomial) time, see [2] for details. Other complexity classes may be defined from these ones using relativized computations. If \mathcal{C} and \mathcal{D} are complexity classes and $A \subseteq \mathbb{R}^\infty$, we denote by \mathcal{C}^A the class of subsets decided by machines in \mathcal{C} using A as an oracle and we denote

$$\mathcal{C}^{\mathcal{D}} = \bigcup_{S \in \mathcal{D}} \mathcal{C}^S.$$

Definition 2.1 Let $A \subseteq \mathbb{R}^\infty$. We define inductively the class $PH_{\mathbb{R}}^A$ as follows:

$$\begin{aligned} \Sigma_{\mathbb{R}}^{0,A} &= \Pi_{\mathbb{R}}^{0,A} &= P_{\mathbb{R}}^A \\ \Sigma_{\mathbb{R}}^{i+1,A} &= NP_{\mathbb{R}}^{(\Sigma_{\mathbb{R}}^i A)} &= NP_{\mathbb{R}}^{(\Pi_{\mathbb{R}}^i A)} \\ \Pi_{\mathbb{R}}^{i+1,A} &= coNP_{\mathbb{R}}^{(\Sigma_{\mathbb{R}}^i A)} &= coNP_{\mathbb{R}}^{(\Pi_{\mathbb{R}}^i A)}, \end{aligned}$$

with

$$\text{PH}_{\mathbb{R}}^A = \bigcup_{i \in \mathbb{N}} \Sigma_{\mathbb{R}}^{i,A} = \bigcup_{i \in \mathbb{N}} \Pi_{\mathbb{R}}^{i,A}.$$

Note that this is equivalent to defining $\Sigma_{\mathbb{R}}^{i+1,A}$ as $(\text{NP}_{\mathbb{R}}^A)^{(\Sigma_{\mathbb{R}}^{i,A})}$. Indeed, since $A \subseteq \Sigma_{\mathbb{R}}^{i,A}$, an oracle query to A in $\text{NP}_{\mathbb{R}}^A$ can be considered to be an oracle query to $\Sigma_{\mathbb{R}}^{i,A}$, hence

$$(\text{NP}_{\mathbb{R}}^A)^{(\Sigma_{\mathbb{R}}^{i,A})} \subseteq \text{NP}_{\mathbb{R}}^{(\Sigma_{\mathbb{R}}^{i,A})}.$$

Definition 2.1 naturally induces an unambiguous definition of the levels of $\text{QH}_{\mathbb{R}}$ described in the introduction.

We now focus on formally defining the notion of quantifier prefix, and the corresponding prefix complexity classes.

Definition 2.2 A *quantifier block* \mathcal{Q} is one of the following functions which, given $n \in \mathbb{N}$ produce:

$$\begin{aligned} B_E(n) &= \exists y_1 \in \{0, 1\}, \forall y_2 \in \{0, 1\} \cdots Q y_n \in \{0, 1\}, \\ B_A(n) &= \forall y_1 \in \{0, 1\}, \exists y_2 \in \{0, 1\} \cdots \overline{Q} y_n \in \{0, 1\}, \\ \exists_{\mathbb{R}}(n) &= \exists (y_1, \dots, y_n) \in \mathbb{R}^n, \text{ or} \\ \forall_{\mathbb{R}}(n) &= \forall (y_1, \dots, y_n) \in \mathbb{R}^n, \end{aligned}$$

where $Q = \exists, \overline{Q} = \forall$ if n is odd and $Q = \forall, \overline{Q} = \exists$ otherwise. For such a quantifier block \mathcal{Q}^i , and $n \in \mathbb{N}$, we denote by y^i the corresponding quantified sequence (y_1^i, \dots, y_n^i) . We say that a block is *real* if it is either $\exists_{\mathbb{R}}$ or $\forall_{\mathbb{R}}$ and that it is *digital* if it is either B_E or B_A . We sometimes write simply B to denote one of the latter two.

A *quantifier prefix* \mathcal{P} of depth k is a sequence of quantifier blocks $\mathcal{Q}^1 \cdots \mathcal{Q}^k$ with $\mathcal{Q}^i \neq \mathcal{Q}^{i+1}$ for $i = 1, \dots, k-1$ and no two consecutive digital blocks. It is said to be *purely real* if its blocks are only $\exists_{\mathbb{R}}$ and $\forall_{\mathbb{R}}$. Its *complementary prefix* is $\overline{\mathcal{Q}}^1 \cdots \overline{\mathcal{Q}}^k$, where $\overline{B_A} = B_E$, $\overline{B_E} = B_A$, $\overline{\exists_{\mathbb{R}}} = \forall_{\mathbb{R}}$ and $\overline{\forall_{\mathbb{R}}} = \exists_{\mathbb{R}}$.

Quantifier prefixes can be (and historically have been) naturally related to complexity classes.

Definition 2.3 Let $A \subseteq \mathbb{R}^\infty$, $f : \mathbb{N} \rightarrow \mathbb{N}$ a function, and $\mathcal{P} = \mathcal{Q}^1 \cdots \mathcal{Q}^k$ a quantifier prefix. We define

$$\mathcal{P}(A, f) = \{x \in \mathbb{R}^\infty \mid \mathcal{Q}^1(f(|x|)) \cdots \mathcal{Q}^k(f(|x|)), (x, y^1, \dots, y^k) \in A\}.$$

For a complexity class \mathcal{C} over \mathbb{R} and a class \mathcal{F} of functions we define the prefix class

$$\mathcal{P}(\mathcal{C}, \mathcal{F}) = \bigcup_{\substack{A \in \mathcal{C} \\ f \in \mathcal{F}}} \mathcal{P}(A, f).$$

Denote by **Poly** the class of polynomial functions and by **Exp** the class of exponential functions (i.e., of the form 2^f for $f \in \text{Poly}$). It follows from Definition 2.3 that $\text{DPAT}_{\mathbb{R}} = B(\text{P}_{\mathbb{R}}, \text{Poly})$, $\text{PH}_{\mathbb{R}} = \bigcup_{\mathcal{P}} \mathcal{P}(\text{P}_{\mathbb{R}}, \text{Poly})$ for purely real \mathcal{P} , $\text{NPAR}_{\mathbb{R}} = \exists_{\mathbb{R}}(\text{PAR}_{\mathbb{R}}, \text{Poly})$, $\text{coNPAR}_{\mathbb{R}} = \forall_{\mathbb{R}}(\text{PAR}_{\mathbb{R}}, \text{Poly})$, $\text{NPAR}_{\mathbb{R}}^* = \exists_{\mathbb{R}}(\text{PAR}_{\mathbb{R}}, \text{Exp})$, and $\text{coNPAR}_{\mathbb{R}}^* = \forall_{\mathbb{R}}(\text{PAR}_{\mathbb{R}}, \text{Exp})$.

Further relations between complexity classes and quantifiers are obtained by allowing sequences of prefixes of variable depth.

Definition 2.4 We say that $f : \mathbb{N} \rightarrow \mathbb{N}$ is *polynomially constructible* when, for all $n \in \mathbb{N}$, $f(n)$ is bounded by—and can be computed in time bounded by—a polynomial in n .

Definition 2.5 Let $\mathcal{P}_* = \{\mathcal{P}_n\}_{n \in \mathbb{N}}$ be a sequence of quantifier prefixes. We say that \mathcal{P}_* is *uniform* when there exists a Turing machine which, given n , writes down \mathcal{P}_n in time polynomial in n . For such a sequence and a polynomially constructible function $f : \mathbb{N} \rightarrow \mathbb{N}$ we define

$$\mathcal{P}_*(A, f) = \{x \in \mathbb{R}^{\infty} \mid x \in \mathcal{P}_{|x|}(A, f)\}$$

and, for classes \mathcal{C} and \mathcal{F} ,

$$\mathcal{P}_*(\mathcal{C}, \mathcal{F}) = \bigcup_{\substack{A \in \mathcal{C} \\ f \in \mathcal{F}}} \mathcal{P}_*(A, f).$$

Denote by **Const** the class of constant functions. We then have $\text{PAT}_{\mathbb{R}} = \bigcup_{p \in \text{Poly}} \mathcal{P}_*(\text{P}_{\mathbb{R}}, \text{Const})$ where \mathcal{P}_n is purely real of depth $p(n)$ beginning, say, with $\exists_{\mathbb{R}}$.

3 Nondeterministic parallelism

The following result goes back to [10].

Proposition 3.1 [2, §19.2, Th. 1] *There is a universal constant $\gamma > 0$ such that, for every $S \subseteq \mathbb{R}^n$ and every algebraic circuit \mathcal{C} deciding S , the*

depth t of \mathcal{C} satisfies

$$t \geq \gamma \left(\sqrt{\frac{\log(\# \text{c.c.}(S))}{n}} \right)$$

where $\# \text{c.c.}(S)$ denotes the number of connected components of S . \square

Proposition 3.2 $\text{PAR}_{\mathbb{R}} \subsetneq \text{DNP}\text{AR}_{\mathbb{R}}^*$.

PROOF. Consider the set

$$S = \{x \in \mathbb{R}^\infty \mid x_1 \in \{0, 1, \dots, 2^{2^{|x|}} - 1\}\}.$$

The following algorithm decides S within $\text{DNP}\text{AR}_{\mathbb{R}}^*$,

```

input  $x \in \mathbb{R}^n$ 
guess  $b_0, \dots, b_{2^n-1} \in \{0, 1\}$ 
  for  $i = 0, \dots, 2^n - 1$  in parallel do
    compute  $z_i := 2^i$ 
  end for
  compute  $y = \sum_{i=0}^{2^n-1} b_i z_i$ 
  if  $x_1 = y$  then ACCEPT else REJECT

```

But the subset $S_n = \{x \in S \mid |x| = n\}$ has 2^{2^n} connected components and hence, it follows from Proposition 3.1 that S can not be decided in parallel polynomial time. \square

Definition 3.3 Let $P = P_1, \dots, P_t \in \mathbb{R}[X_1, \dots, X_k]$ be a set of real polynomials. A *sign condition* over P is a tuple $\theta \in \{-1, 0, 1\}^t$. We say that θ is *realizable by* P if and only if there exists $(x_1, \dots, x_k) \in \mathbb{R}^k$ such that

$$\theta = (\text{sign}(P_1(x_1, \dots, x_k)), \dots, \text{sign}(P_t(x_1, \dots, x_k))).$$

We write

$$\text{SIGN}(P_1, \dots, P_s) = \{(\text{sign}(P_1(x)), \dots, \text{sign}(P_s(x))) \mid x \in \mathbb{R}^k\},$$

the set of sign conditions realizable by P_1, \dots, P_s .

The following result is a special case of [1, Th. 1.3.4].

Theorem 3.4 Let $P_1, \dots, P_t \in \mathbb{R}[X_1, \dots, X_k]$ be real polynomials of degree at most d . Then, the size of the set $\text{SIGN}(P_1, \dots, P_t)$ is bounded by $t^k d^{\mathcal{O}(k)}$. Moreover, there exists an algorithm which, given $P_1, \dots, P_t \in \mathbb{R}[X_1, \dots, X_k]$ of degree at most d , computes $\text{SIGN}(P_1, \dots, P_t)$ in parallel time $(k(\log(t) + \log(d)))^{\mathcal{O}(1)}$ with $t^k d^{\mathcal{O}(k)}$ processors. \square

Proposition 3.5 $\text{NPAR}_{\mathbb{R}} \subseteq \text{PAR}_{\mathbb{R}}$.

PROOF. Let $\mathcal{L} \in \text{NPAR}_{\mathbb{R}}$. Then there exists $\mathcal{L}' \in \text{PAR}_{\mathbb{R}}$ and a polynomial p such that, for $x \in \mathbb{R}^n$, $x \in \mathcal{L}$ if and only if there exists $y \in \mathbb{R}^{p(n)}$ with $(x, y) \in \mathcal{L}'$. Since $\mathcal{L}' \in \text{PAR}_{\mathbb{R}}$, \mathcal{L}' may be decided by a P-uniform family of arithmetic circuits $\mathcal{C}_n, n \in \mathbb{N}$, of polynomial depth $q(n)$.

Consider $x = (x_1, \dots, x_n) \in \mathbb{R}^n$, and denote by \mathcal{C}_x the circuit \mathcal{C}_n , where the n first input nodes are labeled with (x_1, \dots, x_n) , and the last $p(n)$ by variables $Y_1, \dots, Y_{p(n)}$. Then $x \in \mathcal{L}$ if and only if the semi-algebraic set $S_x \subseteq \mathbb{R}^{p(n)}$ decided by \mathcal{C}_x is non-empty.

Let us denote by $\text{depth}(t)$ the depth of a node t in \mathcal{C}_x , and define inductively the *sign-depth* $\text{sdepth}(t)$ of a node t in S_x as follows:

- (i) If t is an input node then $\text{sdepth}(t) = 0$.
- (ii) If t is a computation node with parent nodes t^l and t^r , then $\text{sdepth}(t) = \max\{\text{sdepth}(t^l), \text{sdepth}(t^r)\}$.
- (iii) If t is a sign node with parent node t' , then $\text{sdepth}(t) = \text{sdepth}(t') + 1$.

Denote by S_x the set of sign nodes of \mathcal{C}_x , and by $S_i, i \leq q(n)$, its set of sign nodes of sign depth at most i . Clearly,

$$S_1 \subseteq S_2 \subseteq \dots \subseteq S_{q(n)} = S_x.$$

Let t be a sign node of \mathcal{C}_x of sign-depth $d > 1$. Define \mathcal{C}_t to be the sub-circuit of \mathcal{C}_x consisting of all the ancestor nodes t' of t with sign-depth less than d , and such that no sign node other than t or t' occurs along the path $t' \rightarrow \dots \rightarrow t$. Then, \mathcal{C}_t is an arithmetic circuit without inner sign nodes, and whose input nodes are taken from the x_i 's, the Y_i 's, and the sign nodes in S_{d-1} . Assume $\theta = (\theta_1, \dots, \theta_{|S_{d-1}|}) \in \{-1, 0, 1\}^{|S_{d-1}|}$ is a fixed sign condition for the sign nodes of S_{d-1} . Given $\theta = (\theta_1, \dots, \theta_{|S_{d-1}|})$, \mathcal{C}_t computes a polynomial $P_t^\theta \in \mathbb{R}[Y_1, \dots, Y_{p(n)}]$ of degree at most $2^{\text{depth}(t)}$. If t is the j th sign node in S_d we denote this polynomial by P_j^θ .

Similarly, to a sign node t of sign-depth 1 corresponds a circuit \mathcal{C}_t , which computes a polynomial $P_t \in \mathbb{R}[Y_1, \dots, Y_{p(n)}]$ of degree at most $2^{\text{depth}(t)}$.

Let us now define inductively the following sets,

$$\text{SIGN}^1 = \text{SIGN}(P_1, \dots, P_{|S_1|})$$

and, for $d > 0$,

$$\text{SIGN}^{d+1} = \bigcup_{\theta \in \text{SIGN}^d} \text{SIGN}(P_1^\theta, \dots, P_{|S_{d+1}|}^\theta).$$

Denote by **output** the output node of \mathcal{C}_x which, without loss of generality, can be considered to be a sign node.

Consider now the following parallel algorithm

```

input  $x \in \mathbb{R}^n$ 
for  $d = 1$  to  $q(n)$  do
    compute  $S_d$ ,
for  $d = 1$  to  $q(n)$  do
    compute  $\text{SIGN}^d$  from  $\text{SIGN}^{d-1}$ ,
    check whether  $\exists \theta \in \text{SIGN}^{q(n)}, \theta_{\text{output}} = 1$ ,
    and accept or reject accordingly.

```

We now prove that this algorithm decides \mathcal{L} within the time and processor bounds required.

For $d \leq q(n)$, we say that a sign condition θ over the sign nodes of S_d is effectively realizable if and only if it is realizable by the polynomials $P_1^\theta, \dots, P_{|S_d|}^\theta$.

Claim 1: $\text{SIGN}^{q(n)}$ is the set of signs conditions over the signs nodes of S_x which are effectively realizable.

The proof follows an easy induction on d .

Claim 2: The algorithm above decides \mathcal{L} .

By claim 1, all effectively realizable sign conditions over the sign nodes are contained in $\text{SIGN}^{q(n)}$. Moreover, an existential witness $(y_1, \dots, y_{p(n)})$ is accepting if and only if the sign of the output node is 1 in the corresponding realizable sign condition.

Claim 3: The algorithm works in parallel time $(p(n)q(n))^{\mathcal{O}(1)}$ with $2^{q(n)\mathcal{O}(p(n)q(n))} = 2^{\mathcal{O}(p(n)q(n))}$ processors.

Indeed, the computation of S_d is clearly doable in parallel time $\mathcal{O}(q(n))$ with at most $2^{\mathcal{O}(q(n))}$ processors. Now, by induction on d we prove that SIGN^d has size at most $2^{d\mathcal{O}(p(n)q(n))}$, and is computable in time $(p(n)q(n))^{\mathcal{O}(1)}$ with at most $2^{d\mathcal{O}(p(n)q(n))}$ processors.

Note that, for all $d \leq q(n)$, $|S_d| \leq 2^{q(n)}$, and the degree of all polynomials is also bounded by $2^{q(n)}$.

For $d = 1$, it follows from Theorem 3.9.

Now, given SIGN^{d-1} , by Theorem 3.9 again, the size of SIGN^d is bounded by $|\text{SIGN}^{d-1}|2^{\mathcal{O}(p(n)q(n))}$, and SIGN^d is computable in parallel time $(p(n)q(n))^{\mathcal{O}(1)}$ with $|\text{SIGN}^{d-1}|2^{\mathcal{O}(p(n)q(n))}$ processors, by performing the computation in parallel for all $\theta \in \text{SIGN}^{d-1}$.

The sequential composition of these parallel algorithms yields an algorithm computing $\text{SIGN}^{q(n)}$ in time $(p(n)q(n))^{\mathcal{O}(1)}$ with less than $2^{q(n)\mathcal{O}(p(n)q(n))}$ processors.

Eventually, checking in parallel whether $\exists \theta \in \text{SIGN}^{q(n)}$, $\theta_{\text{output}} = 1$ can also be performed within the same time bound, with the same number of processors, from which the bounds for the whole algorithm follow. \square

The following result can be seen as a real version of Savitch's Theorem [9].

Theorem 3.6 $\text{NPAR}_{\mathbb{R}} = \text{PAR}_{\mathbb{R}} = \text{coNPAR}_{\mathbb{R}}$.

PROOF. The inclusion $\text{NPAR}_{\mathbb{R}} \subseteq \text{PAR}_{\mathbb{R}}$ is shown in Proposition 3.5. The reversed inclusion is trivial. This shows the first equality. The second now follows since $\text{PAR}_{\mathbb{R}}$ is also closed under complement. \square

Realizable sign conditions correspond to (real) existential quantifiers (for a certain specific predicate). One may extend this notion to alternating quantifiers. The extension of Proposition 3.5 thus obtained, Proposition 3.10 below, will be useful to us.

Definition 3.7 Let $P = P_1, \dots, P_t \in \mathbb{R}[X_1, \dots, X_k]$ and $l, s \in \mathbb{N}$ such that $ls = k$. Denote, for $i = 1, \dots, l$, $\mathbf{y}^i = (y_1^i, \dots, y_s^i)$. To l, s , and P , we associate a sequence of list of sign conditions as follows. For $\bar{\mathbf{y}} = (\mathbf{y}^l, \dots, \mathbf{y}^1)$ we let

$$\text{SIGN}_0(l, s, P)(\bar{\mathbf{y}}) = \{(\text{sign}(P_1(\bar{\mathbf{y}})), \dots, \text{sign}(P_t(\bar{\mathbf{y}})))\}$$

and for $j > 0$ and $\overline{\mathbf{y}^{[j]}} = (\mathbf{y}^l, \dots, \mathbf{y}^{j+1}) \in \mathbb{R}^s$ we let

$$\text{SIGN}_j(l, s, P)(\overline{\mathbf{y}^{[j]}}) = \left\{ \text{SIGN}_{j-1}(l, s, P)(\overline{\mathbf{y}^{[j]}}) \mid \mathbf{y}^j \in \mathbb{R}^s \right\}.$$

Finally, we define $\text{SIGN}(l, s, P) = \text{SIGN}_l(l, s, P)(\emptyset)$. If l and s are clear from the context we write $\text{SIGN}(P)$.

Remark 3.8 The lists of signs in Definition 3.7 are useful in the context of deciding quantified formulas with quantifiers of the same size. For

$(z_1, \dots, z_t) \in \mathbb{R}^t$, let $\mathcal{F}(z_1, \dots, z_t)$ be a first-order (quantifier free) formula with atoms of the form $(z_i < 0)$, $(z_i = 0)$ or $(z_i > 0)$.

Let $l, s \in \mathbb{N}$ be such that $ls = k$ and $\mathcal{P} = \mathcal{Q}_l \cdots \mathcal{Q}_1$ be a purely real prefix. As above, denote, for $i = 1, \dots, l$, $\mathbf{y}^i = (y_1^i, \dots, y_s^i)$ and let $\bar{\mathbf{y}} = (\mathbf{y}^l, \dots, \mathbf{y}^1)$.

For $P = P_1, \dots, P_t \in \mathbb{R}[X_1, \dots, X_k]$, consider the sentence \mathcal{G} given by

$$\mathcal{Q}_l(s) \cdots \mathcal{Q}_1(s) \mathcal{F}(P_1(\bar{\mathbf{y}}), \dots, P_t(\bar{\mathbf{y}})).$$

Then, for all sign condition $\theta \in \{-1, 0, 1\}^t$ over P_1, \dots, P_t , for all $\bar{\mathbf{y}} \in \mathbb{R}^k$ such that $\theta = (\text{sign}(P_1[\bar{\mathbf{y}}]), \dots, \text{sign}(P_t[\bar{\mathbf{y}}]))$, any atom of \mathcal{F} has the same boolean value in $\mathcal{F}(\theta)$ and in $\mathcal{F}(P_1(\bar{\mathbf{y}}), \dots, P_t(\bar{\mathbf{y}}))$, and therefore

$$\mathcal{F}(\theta) \iff \mathcal{F}(P_1(\bar{\mathbf{y}}), \dots, P_t(\bar{\mathbf{y}})).$$

It follows that the truth or falsity of \mathcal{G} can be decided by simply quantifying over realizable sign conditions over P_1, \dots, P_t instead of quantifying over \mathbb{R}^k , as follows. Define inductively the relation \models :

$$\text{SIGN}_0(P)(\bar{\mathbf{y}}) \models \mathcal{G} \iff \text{SIGN}_0(P)(\bar{\mathbf{y}}) = \{\theta\} \text{ and } \mathcal{F}(\theta)$$

and, for $j > 0$,

$$\text{SIGN}_j(P)(\bar{\mathbf{y}}^{[j]}) \models \mathcal{G} \iff \begin{cases} \mathcal{Q}_j = \forall_{\mathbb{R}} \text{ and } \forall S \in \text{SIGN}_j(P)(\bar{\mathbf{y}}^{[j]}), S \models \mathcal{G} \\ \mathcal{Q}_j = \exists_{\mathbb{R}} \text{ and } \exists S \in \text{SIGN}_j(P)(\bar{\mathbf{y}}^{[j]}), S \models \mathcal{G}. \end{cases}$$

Then, \mathcal{G} is true if and only if $\text{SIGN}(P) \models \mathcal{G}$.

The following extension of Theorem 3.4 is also a special case of [1, Th. 1.3.4].

Theorem 3.9 *Let $P = \{P_1, \dots, P_t \in \mathbb{R}[X_1, \dots, X_k]\}$ be a set of real polynomials of degree at most d , and let $l \in \mathbb{N}, s \in \mathbb{N}$ with $k = ls$.*

Then, the size of the set $\text{SIGN}(l, s, P)$ is bounded by $t^{(s+1)^l} d^{\mathcal{O}(s^l)}$. Moreover, there exists an algorithm which, given $P = \{P_1, \dots, P_t\}$ of degree at most d , l and s , computes $\text{SIGN}(l, s, P)$ in parallel time $(s^l(\log(t) + \log(d)))^{\mathcal{O}(1)}$ with $t^{(s+1)^l} d^{\mathcal{O}(s^l)}$ processors. \square

Proposition 3.10 *Let $\ell : \mathbb{N} \rightarrow \mathbb{N}$ and $s : \mathbb{N} \rightarrow \mathbb{N}$ be polynomially constructible, $s \geq 2$, and let $\mathcal{P}_* = \{\mathcal{P}_n\}_{n \in \mathbb{N}}$ be a uniform sequence of purely real prefixes of depth $\ell(n)$. Then, $\mathcal{L} \in \mathcal{P}_*(\text{PAR}_{\mathbb{R}}, s)$ can be decided in deterministic parallel time $(s(n)^{\ell(n)} n)^{\mathcal{O}(1)}$ with $2^{n\mathcal{O}(s(n)^{\ell(n)})}$ processors.*

PROOF. The proof follows essentially that of Proposition 3.5 (with Theorem 3.9 replacing Theorem 3.4).

Let $\mathcal{L} \in \mathcal{P}_*(\text{PAR}_{\mathbb{R}}, s)$. Then there exists $\mathcal{L}' \in \text{PAR}_{\mathbb{R}}$ such that

$$\mathcal{L} = \mathcal{P}_*(\mathcal{L}', s).$$

Since $\mathcal{L}' \in \text{PAR}_{\mathbb{R}}$, \mathcal{L}' may be decided by a P-uniform family of arithmetic circuits $\mathcal{C}_n, n \in \mathbb{N}$, of polynomial depth $q(n)$.

Consider $x = (x_1, \dots, x_n) \in \mathbb{R}^n$, and denote by \mathcal{C}_x the circuit \mathcal{C}_n , where the n first input nodes are labeled with (x_1, \dots, x_n) , and the last $s(n)\ell(n)$ by variables $Y_1^{\ell(n)}, \dots, Y_{s(n)}^{\ell(n)}, \dots, Y_1^1, \dots, Y_{s(n)}^1$.

For $(y_1^i, \dots, y_{s(n)}^i) \in \mathbb{R}^{s(n)}$, we use the notation $\mathbf{y}^i = (y_1^i, \dots, y_{s(n)}^i)$. Assume $\mathcal{P}_n = \mathcal{Q}_{\ell(n)}, \dots, \mathcal{Q}_1$. Then, $x \in \mathcal{L}$ if and only if

$$\mathcal{Q}_{\ell(n)}(s(n)) \cdots \mathcal{Q}_1(s(n)) \mathcal{C}_x \text{ accepts } (\mathbf{y}^{\ell(n)}, \dots, \mathbf{y}^1).$$

Using similar notations as in the proof of Proposition 3.5, for a given nested list of signs $\text{SIGN}(l, s, P)$ and a sign condition θ over P , define inductively the relation \sqsubseteq as follows:

$$\theta \sqsubseteq \text{SIGN}_0(\bar{\mathbf{y}}) \iff \text{SIGN}_0(\bar{\mathbf{y}}) = \{\theta\}$$

and, for $j > 0$,

$$\theta \sqsubseteq \text{SIGN}_j(\overline{\mathbf{y}^{[j]}}) \iff \exists S \in \text{SIGN}_j(\overline{\mathbf{y}^{[j]}}), \theta \sqsubseteq S.$$

Now, define inductively the following sets:

$$\text{SIGN}^1 = \text{SIGN}(\ell(n), s(n), P_1, \dots, P_{|S_1|})$$

and, for $d > 1$,

$$\text{SIGN}^d = \bigcup_{\theta \sqsubseteq \text{SIGN}^{d-1}} \left\{ \text{SIGN} \left(\ell(n), s(n), P_1^\theta, \dots, P_{|S_d|}^\theta \right) \right\}.$$

Denote by **output** the output node of \mathcal{C}_x which, without loss of generality, can be considered to be a sign node, and define inductively the relation \models by

$$\text{SIGN}_0^{q(n)}(\mathbf{y}^{\ell(n)}, \dots, \mathbf{y}^1) = \{\theta\} \models \mathcal{C}_x \iff \theta_{\text{output}} = 1$$

and, for $j > 0$ and $\overline{\mathbf{y}^{[j]}} = (\mathbf{y}^{\ell(n)}, \dots, \mathbf{y}^{j+1})$,

$$\text{SIGN}_j^{q(n)}(\overline{\mathbf{y}^{[j]}}) \models \mathcal{C}_x \iff \begin{cases} \mathcal{Q}_j = \forall_{\mathbb{R}} & \text{and } \forall S \in \text{SIGN}_j^{q(n)}(\overline{\mathbf{y}^{[j]}}), S \models \mathcal{C}_x \\ \mathcal{Q}_j = \exists_{\mathbb{R}} & \text{and } \exists S \in \text{SIGN}_j^{q(n)}(\overline{\mathbf{y}^{[j]}}), S \models \mathcal{C}_x. \end{cases}$$

Consider now the following parallel algorithm

```

input  $x \in \mathbb{R}^n$ 
for  $d = 1$  to  $q(n)$  do
  compute  $S_d$ ,
for  $d = 1$  to  $q(n)$  do
  compute  $\text{SIGN}^d$  from  $\text{SIGN}^{d-1}$ ,
  check whether  $\text{SIGN}^{q(n)} \models \mathcal{C}_x$ ,
  and accept or reject accordingly.

```

Then, following the proof of Proposition 3.5 and Remark 3.8, the algorithm above decides \mathcal{L} within the time and processor bounds required. \square

4 Parallel polynomial time and quantifier prefixes

We next use the results in the previous section to characterize quantifier prefixes both decidable in $\text{PAR}_{\mathbb{R}}$ and undecidable in $\text{PAR}_{\mathbb{R}}$.

4.1 Prefixes in $\text{PAR}_{\mathbb{R}}$

Lemma 4.1 *For any quantifier prefix \mathcal{P}*

$$\text{P}_{\mathbb{R}}^{\mathcal{P}(\text{P}_{\mathbb{R}}, \text{Poly})} \subseteq B\mathcal{P}\overline{\mathcal{P}}(\text{P}_{\mathbb{R}}, \text{Poly}),$$

where, moreover, the B block contains only existential digital quantifiers.

PROOF. Let $\mathcal{P} = \mathcal{Q}^1 \dots \mathcal{Q}^k$ and let $\mathcal{L} \in \text{P}_{\mathbb{R}}^{\mathcal{P}(\text{P}_{\mathbb{R}}, \text{Poly})}$. Then, there exists $\mathcal{L}' \in \mathcal{P}(\text{P}_{\mathbb{R}}, \text{Poly})$ such that $\mathcal{L} \in \text{P}_{\mathbb{R}}^{\mathcal{L}'}$. It follows from Definition 2.2 that there exists a machine M , polynomials p, p' and $\mathcal{L}'' \in \text{P}_{\mathbb{R}}$ such that

- (1) M decides $x \in \mathcal{L}$ in time $p(|x|)$ with oracle queries $q_1, \dots, q_{p(|x|)}$ to \mathcal{L}' , where $|q_i| \leq p(|x|)$ for all $i = 1, \dots, p(|x|)$, and
- (2) $q_i \in \mathcal{L}' \iff \mathcal{Q}^1(p'(|x|)) \dots \mathcal{Q}^k(p'(|x|)), (q_i, y_i^1, \dots, y_i^k) \in \mathcal{L}''$ for all $i = 1, \dots, p(|x|)$.

From (2) above, it follows that

$$q_i \notin \mathcal{L}' \iff \overline{\mathcal{Q}^1}(p'(|x|)) \dots \overline{\mathcal{Q}^k}(p'(|x|)) (q_i, y_i^1, \dots, y_i^k) \notin \mathcal{L}''.$$

Consider the following algorithm:

```

input  $x \in \mathbb{R}^n$ 
guess  $z_1, \dots, z_{p(n)} \in \{0, 1\}$ 
  for  $i = 1, \dots, p(n)$  do
    compute the  $i^{th}$  query  $q_i \in \mathbb{R}^{p(n)}$  of  $M$  to  $\mathcal{L}'$ 
    assume the oracle answer is  $z_i$ , and resume the computation of  $M$ 
  end for
if  $M$  rejects then REJECT
else
  (*) for all  $i = 1, \dots, p(n)$  with  $z_i = 1$  do
    check whether  $\mathcal{Q}^1(p'(|x|)) \cdots \mathcal{Q}^k(p'(|x|)) (q_i, y_i^1, \dots, y_i^k) \in \mathcal{L}''$ ,
    and let  $a_i \in \{0, 1\}$  be the answer
  end for all
  (**) for all  $i = 1, \dots, p(n)$  with  $z_i = 0$  do
    check whether  $\overline{\mathcal{Q}^1}(p'(|x|)) \cdots \overline{\mathcal{Q}^k}(p'(|x|)) (q_i, y_i^1, \dots, y_i^k) \notin \mathcal{L}''$ ,
    and let  $a_i \in \{0, 1\}$  be the answer
  end for all
  if  $\exists a_i \neq z_i$  then REJECT else ACCEPT

```

It is clear that the algorithm above decides \mathcal{L} .

In this algorithm, the queries

$$\mathcal{Q}^1(p'(|x|)) \cdots \mathcal{Q}^k(p'(|x|)) (q_i, y_i^1, \dots, y_i^k) \in \mathcal{L}''$$

for all i such that $z_i = 1$ can be merged in a single $\mathcal{P}(\mathbb{P}_{\mathbb{R}}, \text{Poly})$ query, with polynomial bound $p(|x|)p'(|x|)$, by first quantifying over all (y_i^1, \dots, y_i^k) at once, and then sequentially checking $(q_i, y_i^1, \dots, y_i^k) \in \mathcal{L}''$ for all i . Similarly, the queries

$$\overline{\mathcal{Q}^1}(p'(|x|)) \cdots \overline{\mathcal{Q}^k}(p'(|x|)) (q_i, y_i^1, \dots, y_i^k) \notin \mathcal{L}''$$

for all i such that $z_i = 0$ can be merged in a single $\overline{\mathcal{P}}(\mathbb{P}_{\mathbb{R}}, \text{Poly})$ query, with polynomial bound $p(|x|)p'(|x|)$. Now, the existential boolean query over the z_i , the $\mathcal{P}(\mathbb{P}_{\mathbb{R}}, \text{Poly})$ query and the $\overline{\mathcal{P}}(\mathbb{P}_{\mathbb{R}}, \text{Poly})$ query can all be merged into a single query, for instance by sequentially composing them.

It follows that the algorithm above is in $B\mathcal{P}\overline{\mathcal{P}}(\mathbb{P}_{\mathbb{R}}, \text{Poly})$. Therefore,

$$\mathbb{P}_{\mathbb{R}}^{\mathcal{P}(\mathbb{P}_{\mathbb{R}}, \text{Poly})} \subseteq B\mathcal{P}\overline{\mathcal{P}}(\mathbb{P}_{\mathbb{R}}, \text{Poly}). \quad \square$$

Remark 4.2 Since the variables queried in steps (*) and (**) in the algorithm of Lemma 4.1 do not occur in the same computation, their prefixes \mathcal{P} and $\overline{\mathcal{P}}$ can be merged in a way much more concise than $\mathcal{P}\overline{\mathcal{P}}$.

- (1) if \mathcal{P} is purely real beginning with $\forall_{\mathbb{R}}$, one can merge them as $\exists_{\mathbb{R}}\mathcal{P}$.
- (2) if \mathcal{P} contains exactly k (maximal) B blocks, \mathcal{P} and $\overline{\mathcal{P}}$ can be merged in a prefix \mathcal{P}'' with exactly k (maximal) B blocks.

Lemma 4.1 together with Remark 4.2 yield the following characterization of complexity classes (of which (i) is already a well-known result and (iv) is in [4]).

Corollary 4.3 (i) $\Sigma_{\mathbb{R}}^i = \mathcal{P}(\mathbb{P}_{\mathbb{R}}, \text{Poly})$, where \mathcal{P} consists in i alternations of $\exists_{\mathbb{R}}$ and $\forall_{\mathbb{R}}$ blocks, beginning with $\exists_{\mathbb{R}}$.

- (i) $\mathbb{P}_{\mathbb{R}}^{\text{DPAT}} = \text{DPAT}_{\mathbb{R}}$.
- (iii) $\text{PH}_{\mathbb{R}}^{\text{DPAT}_{\mathbb{R}}} = \{\mathcal{P}(\mathbb{P}_{\mathbb{R}}, \text{Poly}) \mid \mathcal{P} = \mathcal{P}'B \text{ with } \mathcal{P}' \text{ purely real}\}$.
- (iv) $\text{DPAT}_{\mathbb{R}}^{\text{PH}_{\mathbb{R}}} = \{\mathcal{P}(\mathbb{P}_{\mathbb{R}}, \text{Poly}) \mid \mathcal{P} = B\mathcal{P}' \text{ with } \mathcal{P}' \text{ purely real}\}$.
- (v) $\Theta_i = \{\mathcal{P}(\mathbb{P}_{\mathbb{R}}, \text{Poly}) \mid \mathcal{P} \text{ contains at most } i+1 \text{ (maximal) } B \text{ blocks, and at most } i \text{ (maximal) purely real subprefixes}\}$.
- (vi) $\Upsilon_i = \{\mathcal{P}(\mathbb{P}_{\mathbb{R}}, \text{Poly}) \mid \mathcal{P} \text{ contains at most } i \text{ (maximal) } B \text{ blocks, and at most } i+1 \text{ (maximal) purely real subprefixes}\}$.
- (vii) $\text{QH}_{\mathbb{R}} = \{\mathcal{P}(\mathbb{P}_{\mathbb{R}}, \text{Poly})\}$.

PROOF.

- (i) By induction on i , the base case being $\Sigma_{\mathbb{R}}^0 = \mathbb{P}_{\mathbb{R}}$. Since $\Sigma_{\mathbb{R}}^{i+1} = \exists_{\mathbb{R}}(\mathbb{P}_{\mathbb{R}}^{(\Pi_{\mathbb{R}}^i)}, \text{Poly})$, and, by induction hypothesis, $\Pi_{\mathbb{R}}^i = \overline{\mathcal{P}}(\mathbb{P}_{\mathbb{R}}, \text{Poly})$, $\Sigma_{\mathbb{R}}^i = \mathcal{P}(\mathbb{P}_{\mathbb{R}}, \text{Poly})$ where \mathcal{P} consists in i alternations of $\exists_{\mathbb{R}}$ and $\forall_{\mathbb{R}}$ blocks, beginning with $\exists_{\mathbb{R}}$, we have by Remark 4.2(1) $\Sigma_{\mathbb{R}}^{i+1} = \exists_{\mathbb{R}}(\mathbb{P}_{\mathbb{R}}^{(\Pi_{\mathbb{R}}^i)}, \text{Poly}) = B\exists_{\mathbb{R}}\exists_{\mathbb{R}}\overline{\mathcal{P}}(\mathbb{P}_{\mathbb{R}}, \text{Poly}) = \exists_{\mathbb{R}}\overline{\mathcal{P}}(\mathbb{P}_{\mathbb{R}}, \text{Poly})$, the B block consisting only of boolean existential quantifier being considered as a $\exists_{\mathbb{R}}$ block, and $\exists_{\mathbb{R}}\overline{\mathcal{P}}$ consisting in $i+1$ alternations of $\exists_{\mathbb{R}}$ and $\forall_{\mathbb{R}}$ blocks, beginning with $\exists_{\mathbb{R}}$.
- (ii) $\mathbb{P}_{\mathbb{R}}^{\text{DPAT}} \subseteq \text{DPAT}_{\mathbb{R}}$ by Lemma 4.1, with $\mathcal{P} = B$, the \supseteq inclusion being trivial.
- (iii) We show the statement for $\Sigma_{\mathbb{R}}^i \text{DPAT}_{\mathbb{R}}$, for all $i \geq 0$, by induction on i . The case $i = 0$ follows from Part (ii). The induction step follows from Remark 4.2(1). Assume \mathcal{P} consists only in $\exists_{\mathbb{R}}$ and $\forall_{\mathbb{R}}$ alternating quantifier blocks, beginning with $\exists_{\mathbb{R}}$, then $\mathcal{P}B$ and $\overline{\mathcal{P}}B$ can be merged into $\exists_{\mathbb{R}}\mathcal{P}B$.

- (iv) Immediate from Lemma 4.1
- (v) By induction on i . The base case $\Theta_0 = \text{DPAT}_{\mathbb{R}}$ by definition, the induction following from Remark 4.2(2).
- (vi) By induction on i . The base case $\Gamma_0 = \text{PH}_{\mathbb{R}}$ by Remark 4.2(1), the induction from Remark 4.2(2).
- (vii) Directly from (v) and (vi) above. \square

Theorem 4.4 $\text{QH}_{\mathbb{R}} \subseteq \text{PAR}_{\mathbb{R}}$.

PROOF. Theorem 3.6 yields the first two lines in

$$\begin{aligned} \exists_{\mathbb{R}}(\text{P}_{\mathbb{R}}, \text{Poly}) &\subseteq \exists_{\mathbb{R}}(\text{PAR}_{\mathbb{R}}, \text{Poly}) = \text{NPAR}_{\mathbb{R}} \subseteq \text{PAR}_{\mathbb{R}} \\ \forall_{\mathbb{R}}(\text{P}_{\mathbb{R}}, \text{Poly}) &\subseteq \forall_{\mathbb{R}}(\text{PAR}_{\mathbb{R}}, \text{Poly}) = \text{coNPAR}_{\mathbb{R}} \subseteq \text{PAR}_{\mathbb{R}} \\ B(\text{P}_{\mathbb{R}}, \text{Poly}) &\subseteq B(\text{PAR}_{\mathbb{R}}, \text{Poly}) \subseteq \text{PAR}_{\mathbb{R}}, \end{aligned}$$

the last being simply a matter of enumerating in parallel all possible boolean choices.

By Corollary 4.3(vii), $\text{QH}_{\mathbb{R}} = \{\mathcal{P}(\text{P}_{\mathbb{R}}, \text{Poly})\}$. Therefore, for all $\mathcal{L} \in \text{QH}_{\mathbb{R}}$ there exists a quantifier prefix \mathcal{P} such that $\mathcal{L} \in \mathcal{P}(\text{P}_{\mathbb{R}}, \text{Poly})$. Using the inclusions above, a simple induction on the depth of the quantifier prefix \mathcal{P} shows that $\mathcal{L} \in \text{PAR}_{\mathbb{R}}$. \square

4.2 Prefixes not in $\text{PAR}_{\mathbb{R}}$

We recall the following result originally proved in [5].

Proposition 4.5 [2, §19.1, Prop. 3] *Let $f_n \in \mathbb{R}[X_1, \dots, X_n]$, $n \in \mathbb{N}$, be a family of nonconstant irreducible polynomials such that for each n , the zero set $\mathcal{Z}(f_n)$ is a variety of dimension $n - 1$. Let $d(n) = \deg(f_n)$. Then any parallel machine deciding the set $S = \{x \in \mathbb{R}^{\infty} \mid f_{|x|}(x) = 0\}$ has running time greater than $\log(d(n))$.*

The following Lemma has its origin in a paper by Davenport and Heintz [7].

Lemma 4.6 *Let $\ell : \mathbb{N} \rightarrow \mathbb{N}$ and $s : \mathbb{N} \rightarrow \mathbb{N}$ be polynomially constructible, with $s(n) \geq 2$ for all $n \in \mathbb{N}$. For $n \in \mathbb{N}$ consider the set*

$$\mathcal{S}_n^{\ell, s} = \left\{ (x_1, \dots, x_n) \in \mathbb{R}^n \text{ such that } x_1 + x_2^{2^{s(n)\ell(n)}} = 0 \right\}$$

and let $\mathcal{S}^{\ell,s} = \bigcup_n \mathcal{S}_n^{\ell,s}$.

There exists a uniform sequence $\mathcal{P}^{\ell,s} = \{\mathcal{P}_n^{\ell,s}\}_{n \in \mathbb{N}}$ of prefixes of depth $2\ell(n) + 1$, such that

$$\mathcal{S}^{\ell,s} \in \mathcal{P}^{\ell,s}(\mathbb{P}_{\mathbb{R}}, s + 1).$$

Moreover, each $\mathcal{P}_n^{\ell,s}$ consists in $\ell(n)$ sequences of pairs $\exists_{\mathbb{R}} B$ of size $s(n) + 1$, where the B block has only \forall quantifiers.

PROOF. For $s, d \in \mathbb{N}$, $s \geq 2$, we describe a formula E_s^d over \mathbb{R}^2 such that $E_s^d(x, y)$ expresses that $x = y^{2^{s^d}}$. We may do so inductively by defining $E_s^0(x, y) \equiv (x = y^2)$ and, for $d \geq 1$,

$$\begin{aligned} E_s^d(x, y) &\equiv \exists \gamma_1, \dots, \gamma_{s-1} \in \mathbb{R}, \\ &E_s^{d-1}(x, \gamma_{s-1}) \wedge E_s^{d-1}(\gamma_{s-1}, \gamma_{s-2}) \wedge \dots \wedge E_s^{d-1}(\gamma_1, y). \end{aligned}$$

Indeed, an induction on i shows that, provided E_s^{d-1} expresses that $x = y^{2^{s^{d-1}}}$, $E_s^{d-1}(\gamma_{i+1}, \gamma_i) \wedge \dots \wedge E_s^{d-1}(\gamma_1, y)$ expresses that $\gamma_{i+1} = y^{2^{(i+1)s^{d-1}}}$, and therefore $E_s^d(x, y)$ expresses that $x = y^{2^{s \cdot s^{d-1}}} = y^{2^{s^d}}$.

However, if we unfold such an inductive definition, its length increases by a factor of s at each step of the unfolding, and we eventually get an exponentially long expression. In order to avoid this exponential growth, we introduce the following boolean quantified variables $\mathbf{b} = b_1, \dots, b_{\lceil \log(s+1) \rceil}$, considered as a single natural number ranging from 0 to $s - 1$.

The inductive step in the definition of E_s^d is now as follows:

$$\begin{aligned} E_s^d(x, y) &\equiv \exists \gamma_1^d, \dots, \gamma_{s-1}^d \in \mathbb{R}, \forall \mathbf{b}^d \in \{0, \dots, s-1\}, \exists \alpha^d, \beta^d \in \mathbb{R}, \\ &\left[\left((\alpha^d = x) \wedge (\beta^d = \gamma_{s-1}^d) \wedge (\mathbf{b}^d = 0) \right) \vee \right. \\ &\quad \left((\alpha^d = \gamma_{s-1}^d) \wedge (\beta^d = \gamma_{s-2}^d) \wedge (\mathbf{b}^d = 1) \right) \vee \\ &\quad \vdots \\ &\quad \left. \left((\alpha^d = \gamma_1^d) \wedge (\beta^d = y) \wedge (\mathbf{b}^d = s-1) \right) \right] \wedge \\ &E_s^{d-1}(\alpha^d, \beta^d). \end{aligned}$$

Let us denote by \mathbf{z}_s^d the vector of the quantified variables present in this inductive definition, that is $\mathbf{z}_s^d = (\alpha^d, \beta^d, \gamma_1^d, \dots, \gamma_{s-1}^d, \mathbf{b}^d)$. We define:

$$\begin{aligned} \phi(\mathbf{z}_s^d) \equiv & \left[\left((\alpha^d = x) \wedge (\beta^d = \gamma_{s-1}^d) \wedge (\mathbf{b}^d = 0) \right) \vee \right. \\ & \left((\alpha^d = \gamma_{s-1}^d) \wedge (\beta^d = \gamma_{s-2}^d) \wedge (\mathbf{b}^d = 1) \right) \vee \\ & \vdots \\ & \left. \left((\alpha^d = \gamma_1^d) \wedge (\beta^d = y) \wedge (\mathbf{b}^d = s-1) \right) \right] \end{aligned}$$

The unfolding of the inductive definition of E_s^d can now be written as follows:

$$\begin{aligned} E_s^d(x, y) & \equiv \exists \gamma_1^d, \dots, \gamma_{s-1}^d \in \mathbb{R} \forall \mathbf{b}^d \in \{0, \dots, s-1\} \exists \alpha^d, \beta^d \in \mathbb{R} \\ & \quad \phi(\mathbf{z}_s^d) \wedge E_s^{d-1}(\alpha^d, \beta^d) \\ & \equiv \exists \gamma_1^d, \dots, \gamma_{s-1}^d \in \mathbb{R} \forall \mathbf{b}^d \in \{0, \dots, s-1\} \exists \alpha^d, \beta^d \in \mathbb{R} \\ & \quad \exists \gamma_1^{d-1}, \dots, \gamma_{s-1}^{d-1} \in \mathbb{R} \forall \mathbf{b}^{d-1} \in \{0, \dots, s-1\} \exists \alpha^{d-1}, \beta^{d-1} \in \mathbb{R} \\ & \quad \phi(\mathbf{z}_s^d) \wedge \phi(\mathbf{z}_s^{d-1}) \wedge E_s^{d-1}(\alpha^{d-1}, \beta^{d-1}) \\ & \equiv \\ & \quad \vdots \\ & \equiv \exists \gamma_1^d, \dots, \gamma_{s-1}^d \in \mathbb{R} \dots \exists \alpha^1, \beta^1 \in \mathbb{R} \\ & \quad \phi(\mathbf{z}_s^d) \wedge \dots \wedge \phi(\mathbf{z}_s^1) \wedge E_s^0(\alpha^1, \beta^1). \end{aligned}$$

Note that we let the inner quantifiers migrate in front since the corresponding variables are not used in the previous part of the formula.

Now, to $x = (x_1, \dots, x_n) \in \mathbb{R}^n$, we associate the formula $E_{s(n)}^{\ell(n)}(-x_1, x_2)$. Since $\ell(n)$ and $s(n)$ are computable in time polynomial in n , so is $E_{s(n)}^{\ell(n)}$. Therefore, $E_{s(n)}^{\ell(n)}(-x_1, x_2)$ corresponds to a $\mathcal{P}^{\ell, s}(\mathbb{P}_{\mathbb{R}}, s)$ query with $\mathcal{P}^{\ell, s}$ uniform, $\mathcal{P}_n^{\ell, s}$ of depth $2\ell(n) + 1$, and is true if and only if $x \in \mathcal{S}_{\ell, s}$. \square

Lemma 4.7 *Let $\ell : \mathbb{N} \rightarrow \mathbb{N}$ and $s : \mathbb{N} \rightarrow \mathbb{N}$ be polynomially constructible with $s(n) \geq 2$ for all $n \in \mathbb{N}$, and such that the function*

$$g : n \rightarrow \ell(n) \frac{\log(s(n))}{\log(n+1)}$$

is not bounded. Let $\mathcal{P}_* = \{\mathcal{P}_n\}_{n \in \mathbb{N}}$ be a uniform sequence of prefixes of depth $\ell(n)$. Then,

$$\mathcal{P}_*(\mathbb{P}_{\mathbb{R}}, s+1) \not\subseteq \text{PAR}_{\mathbb{R}}.$$

PROOF. Consider the set $\mathcal{S}^{\ell, s}$ of Lemma 4.6. It is clear that each $f_n[X_1, \dots, X_n] = X_1 + X_2^{2^{s(n)\ell(n)}}$ is irreducible, and that its zero set is a variety of dimension $n-1$. Therefore, by Proposition 4.5, any parallel machine deciding $\mathcal{S}^{\ell, s}$ has running time greater than $s(n)^{\ell(n)}$. Since g is not bounded, $s(n)^{\ell(n)}$ is not polynomially bounded and hence $\mathcal{S}^{\ell, s} \notin \text{PAR}_{\mathbb{R}}$.

For a given prefix \mathcal{P} of depth $d > 1$, define its sequence of alternation $\text{Alt}(\mathcal{P})$ to be the sequence of words in $\{eb, ef, fb\}$ of length $d-1$ such that the i th word is eb (respectively ef , resp. fb) if and only if the i th alternation in \mathcal{P} is between an $\exists_{\mathbb{R}}$ and a B quantifier block, in any order (respectively between an $\exists_{\mathbb{R}}$ and a $\forall_{\mathbb{R}}$ block, resp. between an $\forall_{\mathbb{R}}$ and a B block.)

Furthermore, $\text{Alt}(\mathcal{P})$ contains at least $\lceil \frac{d-1}{3} \rceil$ occurrences of either eb , ef or fb . Denote by $\text{Maj}(\mathcal{P})$ the (lexicographically first) word among eb , ef and fb having more than $\lceil \frac{d-1}{3} \rceil$ occurrences in $\text{Alt}(\mathcal{P})$. Since \mathcal{P}_* is uniform, the function $n \rightarrow \text{Maj}(\mathcal{P}_n)$ is computable in time polynomial in n and, hence, so is the characteristic function of the sets

$$\begin{aligned} EB &= \{n \in \mathbb{N} : \text{Maj}(\mathcal{P}_n) = eb\} \\ EF &= \{n \in \mathbb{N} : \text{Maj}(\mathcal{P}_n) = ef\} \\ FB &= \{n \in \mathbb{N} : \text{Maj}(\mathcal{P}_n) = fb\}. \end{aligned}$$

Since $EB \cup EF \cup FB = \mathbb{N}$, at least one of these sets, that we denote by M , contains infinitely many elements.

Define the sequence of prefixes $\mathcal{P}'_* = \{\mathcal{P}'_n\}_{n \in \mathbb{N}}$ by

$$\mathcal{P}'_n = \begin{cases} \mathcal{P}_n & \text{if } n \in M \\ \emptyset & \text{otherwise.} \end{cases}$$

Clearly \mathcal{P}'_* is uniform. Define now the following set

$$\mathcal{T}_n^{\ell, s} = \begin{cases} \mathcal{S}_n^{\ell, s} & \text{if } n \in M, \text{ and} \\ \emptyset & \text{otherwise,} \end{cases}$$

and let $\mathcal{T}^{\ell, s} = \bigcup_{n \in \mathbb{N}} \mathcal{T}_n^{\ell, s}$. Since M is infinite and $\mathcal{S}^{\ell, s} \notin \text{PAR}_{\mathbb{R}}$ it follows that $\mathcal{T}^{\ell, s} \notin \text{PAR}_{\mathbb{R}}$.

Let $\ell' = \frac{\ell}{12} - 6$. We claim that

$$\begin{aligned} \mathcal{T}^{\ell', s} &\in \mathcal{P}'_*(\mathbb{P}_{\mathbb{R}}, s+1) \text{ if } M = EB \text{ or } EF, \\ (\mathbb{R}^{\infty} \setminus \mathcal{T}^{\ell', s}) &\in \mathcal{P}'_*(\mathbb{P}_{\mathbb{R}}, s+1) \text{ if } M = FB. \end{aligned}$$

Indeed, assume $M = EB$. Then, for $n \in M$, any prefix \mathcal{P}'_n of depth $\ell(n) = 12\ell'(n)$ contains at least $\lceil \frac{\ell(n)}{3} \rceil = 4\ell'(n) + 2$ alternations between $\exists_{\mathbb{R}}$ and B blocks. Therefore, \mathcal{P}'_n contains a subsequence \mathcal{P}'' consisting in $\lceil \frac{\ell(n)}{6} \rceil = 2\ell'(n) + 1$ sequences of pairs $\exists_{\mathbb{R}}, B$. It follows from Lemma 4.6 (consider the blocks not in \mathcal{P}'' as dummy) that $\mathcal{T}^{\ell', s}$ can be decided in $\mathcal{P}'_*(P_{\mathbb{R}}, s + 1)$. Therefore, $\mathcal{P}'_*(P_{\mathbb{R}}, s + 1) \not\subseteq \text{PAR}_{\mathbb{R}}$ and, by construction of \mathcal{P}' , $\mathcal{P}_*(P_{\mathbb{R}}, s + 1) \not\subseteq \text{PAR}_{\mathbb{R}}$.

Similar arguments hold for $M = EF$, where one needs only to replace digital quantifiers in the prefix given by Lemma 4.6 by real ones (since only the universal digital quantifiers of any B block in the prefix of Lemma 4.6 are effectively used). The case $M = FB$ follows by considering the complementary of the prefix given by Lemma 4.6. \square

Corollary 4.8 (i) *Let $\ell : \mathbb{N} \rightarrow \mathbb{N}$ be polynomially constructible and $\mathcal{P}_* = \{\mathcal{P}_n\}_{n \in \mathbb{N}}$ be a uniform sequence of prefixes of depth $\ell(n)$. Then,*

$$\begin{aligned} \mathcal{P}_*(P_{\mathbb{R}}, \text{Poly}) &\subseteq \text{PAR}_{\mathbb{R}} && \text{iff } \ell \text{ is bounded, and} \\ \mathcal{P}_*(\text{PAR}_{\mathbb{R}}, \text{Poly}) &\subseteq \text{PAR}_{\mathbb{R}} && \text{iff } \ell \text{ is bounded.} \end{aligned}$$

(ii) *Let $q : \mathbb{N} \rightarrow \mathbb{N}$ be polynomially constructible and $\mathcal{P}_* = \{\mathcal{P}_n\}_{n \in \mathbb{N}}$ be a uniform sequence of prefixes of depth $\ell(n) = \lceil q(n) \log(n) \rceil$. Then,*

$$\begin{aligned} \mathcal{P}_*(P_{\mathbb{R}}, \text{Const}) &\subseteq \text{PAR}_{\mathbb{R}} && \text{iff } q \text{ is bounded, and} \\ \mathcal{P}_*(\text{PAR}_{\mathbb{R}}, \text{Const}) &\subseteq \text{PAR}_{\mathbb{R}} && \text{iff } q \text{ is bounded.} \end{aligned}$$

PROOF.

- (i) The “if” direction follows from Corollary 4.3 and Theorem 4.4. The “only if” direction follows from Lemma 4.7 with s a polynomial.
- (ii) The “if” direction follows from Proposition 3.10, where one needs only to consider the B blocks as sequences of alternating real quantifiers. The “only if” direction follows from Lemma 4.7 with s a constant. \square

Remark 4.9 (i) An immediate consequence of Corollary 4.8 is $\text{MA}\exists_{\mathbb{R}} \not\subseteq \text{PAR}_{\mathbb{R}}$ and $\text{MA}\forall_{\mathbb{R}} \not\subseteq \text{PAR}_{\mathbb{R}}$ [4].

- (ii) One could also consider the class **Log** of logarithmic functions and wonder on which bounds ℓ for the depth of the blocks yields sets decidable in $\text{PAR}_{\mathbb{R}}$. Lemma 4.7 allows to show that if ℓ grows faster than

$\mathcal{O}\left(\frac{\log n}{\log \log n}\right)$ then $\mathcal{P}_*(\mathbb{P}_{\mathbb{R}}, \mathbf{Log}) \not\subseteq \text{PAR}_{\mathbb{R}}$. Our techniques, though, are not enough to prove the converse.

- (iii) One of the main results in [1] shows that quantified sentences over \mathbb{R} can be decided in parallel time

$$\left(\prod_{j=1}^{\omega} (k_j + 1)\right) \log t + \left(\prod_{j=1}^{\omega} \mathcal{O}(k_j)\right) \log d$$

where ω denotes the number of alternations between $\exists_{\mathbb{R}}$ and $\forall_{\mathbb{R}}$ blocks, k_j the number of variables of the j th block, t the number of polynomials in the quantifier-free predicate and d a bound for their degrees. The $\left(\prod_{j=1}^{\omega} (k_j + 1)\right) \log t$ part of the sum is an upper bound depending on the combinatorial structure of the data, and the second part $\left(\prod_{j=1}^{\omega} \mathcal{O}(k_j)\right) \log d$ is so for its algebraic structure. A variation of Lemma 4.6 and Proposition 4.5 allow us to prove to some extent the optimality of the algebraic part of the bound.

Indeed, given $d, \omega, k_1, \dots, k_{\omega}$, a variation of Lemma 4.6 allows us to express membership to

$$\mathcal{S} = \left\{ (x_1, x_2) \in \mathbb{R}^2 \text{ such that } x_1 + x_2^{d^{\prod k_j}} = 0 \right\}$$

with a quantified sentence over a single polynomial equality of degree $\max\{2d, 4\omega\}$ and with 2ω alternating blocks, the $(2j-1)$ th block of size k_j and the $2j$ th block of size $\log k_j$. Hence, the lower bound obtained from Proposition 4.5 to decide membership in \mathcal{S} , for $d \geq 4\omega$, is of the order of

$$\left(\prod_{j=1}^{\omega} k_j\right) \log d.$$

On the other hand, the first term in the upper bound for the parallel time of the algorithm in [1] vanishes (since $t = 1$) and its second term becomes

$$\left(\prod_{j=1}^{\omega} k_j \log k_j\right) \log d,$$

barely bigger than the lower bound above.

5 Within $\text{NC}_{\mathbb{R}}$

The ideas in the preceding sections may be also applied to parallel computations in polylogarithmic time. We briefly describe how.

Proposition 5.1 *Let $\ell : \mathbb{N} \rightarrow \mathbb{N}$ be polynomially constructible and let $\mathcal{P}_* = \{\mathcal{P}_n\}_{n \in \mathbb{N}}$ be a uniform sequence of prefixes of depth $\ell(n)$. Then,*

$$\mathcal{P}_*(\text{NC}_{\mathbb{R}}^i, \log^j(n)) \subseteq \text{NC}_{\mathbb{R}} \quad \text{iff} \quad \ell \text{ is bounded.}$$

PROOF. The “if” direction follows the proof of Proposition 3.10, with appropriate bounds $\log^j(n)$ for the depth of the circuit \mathcal{C}_x , and $|S_i|$ polynomially bounded for all $i \leq \log^j(n)$. With these bounds, the algorithm given in the proof of Proposition 3.10 works in parallel time $\log(n)^{\mathcal{O}(1)}$ with a polynomial number of processors.

For the “only if” direction, we first remark that, for $j \in \mathbb{N}$, $s : n \mapsto \log(n)^j$ and ℓ bounded, the set $S^{\ell, s}$ of Lemma 4.6 is actually in $\mathcal{P}^{\ell, s}(\text{NC}_{\mathbb{R}}^j, s+1)$ for the same prefix $\mathcal{P}^{\ell, s}$.

Given $j \in \mathbb{N}$ and $s : n \mapsto \log(n)^j$, Proposition 4.5 ensures that $S^{\ell, s} \in \text{NC}_{\mathbb{R}}$ if and only if ℓ is bounded. Then, arguments similar as those developed in the proof of Lemma 4.7 show that, for any uniform sequence \mathcal{P}_* of prefixes of depth $\ell(n)$, $\mathcal{P}_*(\text{NC}_{\mathbb{R}}^j, s+1) \not\subseteq \text{NC}_{\mathbb{R}}$ if ℓ is not bounded. □

References

- [1] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of the ACM*, 43:1002–1045, 1996.
- [2] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer-Verlag, 1998.
- [3] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bulletin of the Amer. Math. Soc.*, 21:1–46, 1989.
- [4] I. Briquel and F. Cucker. A note on parallel and alternating time. *J. of Complexity*, 23:594–602, 2007.
- [5] F. Cucker. $\text{P}_{\mathbb{R}} \neq \text{NC}_{\mathbb{R}}$. *Journal of Complexity*, 8:230–238, 1992.
- [6] F. Cucker. On the complexity of quantifier elimination: the structural approach. *The Computer Journal*, 36:400–408, 1993.

- [7] J.H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *J. Symb. Comput.*, 5:29–35, 1988.
- [8] C. Michaux. Une remarque à propos des machines sur \mathbb{R} introduites par Blum, Shub et Smale. *C. R. Acad. Sci. Paris*, 309, Série I:435–437, 1989.
- [9] Walter J. Savitch. Relationships between nondeterministic and deterministic tape complexities. *J. Comput. Syst. Sci.*, 4(2):177–192, 1970.
- [10] A. Yao. On parallel computation for the knapsack problem. *J. ACM*, 29:898–903, 1982.